

REMARKS

Claims 1-37 are pending and claims 1-37 stand objected to and rejected under 35 USC §§ 101 and 102. The drawings and specification are also objected to and a provisional double-patenting rejection is asserted. Applicant respectfully suggests that the rejections with respect to the claims are traversed in light of the amendments and the following remarks.

Claim Amendments/Corrections

The proposed amendments to the claims include corrections for typographical/grammatical errors that do not add new matter. The proposed amendments also include clarifications that do not add new matter. The clarifications are supported by several portions of the specification including, for example: paragraphs 6, 20-22, 39, and 42.

Drawing Objections

The attached replacement sheet corrects the typographical errors in FIG. 5B. Thus, Applicant respectfully requests that the replacement sheet be entered and the objections be withdrawn.

Specification Objections

The typo in paragraph 21 is corrected and the trademark is corrected to be "MAGIC PACKET™". Thus, Applicant respectfully requests that the amendment be entered and the objection be withdrawn.

Claim Objections

The office action objects to claims 24 and 25 as failing to further limit the independent claim. Applicant respectfully disagrees. Claim 24 indicates that the packet parser is capable of parsing "the wake-on-LAN packet to identify the partition identification" and claim 25 indicates that packet parser is capable of identifying "an extension to the wake-on-LAN packet as the partition identification". Both claims provide more detail about capabilities of the "packet parser" than is described in claim 20 by adding functionality that is not required by claim 20. In

other words, according to claim 20, packet parser does not have to be capable of parsing “wake-on-LAN packet” to identify the partition identification. For instance, if the partition identification were received separately from the packet, which may fall within the scope of claim 20, packet parser would not be required to parse the packet to identify the partition identification in claim 20. The same arguments apply for claim 24.

Similarly, according to claim 20, packet parser does not have to be capable of handling a “wake-on-LAN packet” with an extension attached to identify the partition identification. Thus, Applicant respectfully requests that the objections be withdrawn.

With regards to the objections to claims 8, 9, 10, and 11, these claims are cancelled in the amendments so Applicant respectfully requests that the objections be withdrawn.

Claim rejections under 35 USC § 101

Claims 8-11, 15-19 and 35-37 stand rejected under 35 USC § 101 as being non-statutory subject matter. Applicant cancels 8-11, and 19.

With regards to 15-18 and 35-37, the Office action concludes that signal claims are not patentable subject matter because the claims do not fall into one of the four statutory classes of 35 U.S.C. § 101. Applicants assert that signal claims are in fact statutory subject matter eligible for patent protection. Applicants describe below how courts have consistently found signal claims to be patentable, and expressed principles consistent with these findings. However, notwithstanding our view as to the patentability of signal claims, we are concerned about the inherently transitory nature of signals and the potential for this characteristic of signals to result in ill-defined or overly broad claims. Thus, we also stress the need for strict adherence to the requirements of 35 U.S.C. § 112.

The patentability of signals is not a new concept. The Supreme Court found a claim covering a signal patentable subject matter in 1854 when it upheld such a claim in one of Samuel Morse’s telegraph patents. See *O’Reilly v. Morse*, 56 U.S. 62 (1854).

Signals are articles of manufacture. More recently, the courts have interpreted the term “manufacture” as used in 35 U.S.C. § 101 to mean “the production of articles for use from raw or prepared materials by giving to these materials new forms, qualities, properties or combinations, whether by hand labor or by machinery.” *Diamond v. Chakrabarty*, 447 U.S. 303, at 308, 206

(1980) (quoting *American Fruit Growers, Inc. v. Brogdex Co.*, 283 U.S. 1, 11 (1931)). The USPTO asserts at Annex IV(c), page 56 of the Interim Guidelines that the courts definition of manufacture requires a physical substance, which signals do not have. However, this interpretation is inconsistent with the courts. The Federal Circuit has consistently held that reading limitations into Section 101 regarding subject matter that may be patented where the legislative history does not indicate that Congress clearly intended such limitations is improper. See *In re Alappat*, 33 F.3d 1526, 1542 (Fed. Cir. 1994) (en banc); see also, *State Street. Bank & Trust Co. v. Signature Fin. Group, Inc.*, 149 F.3d 1368, 1373 (Fed. Cir. 1998); *Arrhythmia Research Technology, Inc. v. Corazonix Corp.*, 958 F.2d 1053, 1064 (Fed. Cir. 1992) (Rader, J., concurring).

Furthermore, computer software that is embodied in a signal, whether a carrier wave, baseband, or otherwise, does not fall within any of the three recognized exceptions of patentable subject matter. The signal is not a law of nature, natural phenomenon, or abstract idea. Instead, the signal is an article of manufacture that arises from the practical application of electromagnetic energy.

A signal is also the result of a physical transformation analogous to that found patentable in *Diamond v. Diehr*, 450 U.S. 175 (1981). Electromagnetic energy is transformed from a natural state or some intermediate state to form a data signal. Such a signal is physically different and has undergone a physical transformation from its original state. The key factor is that a physical transformation has occurred - not the extent of the transformation. The resulting signal is the product of a physical transformation which would not exist absent the transformation.

The courts have further construed 35 U.S.C. § 101 as defining patentable subject matter to be that which has a practical application that produces a useful, concrete, and tangible result. See, *State Street. Bank & Trust Co. v. Signature Fin. Group, Inc.*, 149 F.3d 1368, 1373-74 (Fed. Cir. 1998). A signal is a practical application that produces a tangible result. The result of the application of such signals is readily measurable and because it enables the function of the systems in which it is implemented – enables useful results in the operation of the computer systems. A signal, whether transmitted via a wire or wireless technology, can be a unique signal specifically designed to convey specific information or data. A signal is part of the technology

that enables computer-encoded functions to operate. Thus, a signal may transmit process steps so that a useful, concrete and tangible result is achieved (e.g. in a computer).

Additionally, At Annex IV(c), pages 56-57 of the Interim Guidelines, the USPTO further avers that a signal is not a manufacture because it does not fall into the definition of a "manufacture" defined as being a residual class of product in 1 Chisum on Patents, § 1.02[3] (citing W. Robinson, *The Law of Patents for Useful inventions* 270 (1890)). The Office concludes that, "[a] product is a tangible physical article or object, some form of matter, which a signal is not".

However, the tangible nature of a product is not a requirement for patentability under 35 U.S.C. § 101. The Supreme Court did not state that the definition of manufacture under Section 101 requires a tangible article in either *American Fruit Growers* or *Chakrabarty*. Also, as noted above, the Federal Circuit has warned against engrafting additional requirements on to the definition of patentable subject matter under Section 101. But, even if the Office maintains such a tangibility requirement for patentability under Section 101, a signal is a tangible product under any interpretation of such term. According to Webster's' Third New International Dictionary of the English Language Unabridged 2337 (Philip Babcock ed., 1993), tangible means "able to be perceived as materially existent." Signals, albeit transitory in duration, exist in reality and have properties that are physically measurable because they are typically comprised of electron flows that vary over time. See Harry Newton, *Newton's Telecommunications Dictionary* 244 (17th ed. 2001), see also, *A Dictionary of Physics* (John Daintith ed., 2000). Thus, signals may be sensed or perceived using appropriate electronic equipment and its properties can be analyzed and manipulated as desired.

Signals also fall within the definition of computer usable media or computer readable media. A computer is able to detect the signal and recover the computer program embodied therein. It makes no difference whether the computer program is embodied in a physical media such as a hard drive or computer memory or within a data signal. As stated above, a signal is a tangible product that falls within the statutory categories of patentable subject matter. The underlying program is usable by the computer and is thus patentable as reflected in the Interim Guidelines, Annex IV(c), page 57:

[F]rom a technological standpoint, a signal encoded with

functional descriptive material is similar to a computer-readable memory encoded with functional descriptive material, in that they both create a functional interrelationship with a computer. In other words, a computer is able to execute the encoded functions, regardless of whether the format is a disk or a signal.

Therefore, Applicants submit that signal claims fall within at least one of the statutory classes of invention under 35 U.S.C. § 101 whether claimed specifically as a signal or whether claimed as a computer program product. Signal claims are necessary to properly protect and inventor's interest in their invention. Absent such claims, the public would be free to exploit the patentee's invention.

However, because signals are inherently transitory, there is a high degree of risk that claims directed to signals can be drafted in a manner that is indefinite. The scope of these claims must be clear so that the public may understand their metes and bounds in order to determine whether they are infringing. Therefore, when examining signal claims, we caution that examiners must carefully adhere to the requirements for patentability specified in 35 U.S.C. § 112 in determining whether the claimed invention meets all the criteria for patentability.

For example, because one of ordinary skill in the art must be able to practice the invention, it is important to determine that the scope of enablement indicated in the specification is commensurate with the claims in order to prevent overly broad claiming. The examiner should also conduct an intensive review of the written description of each patent application to ensure that the inventor has demonstrated possession of the invention. It may be appropriate to require additional detailed description for signal claims to adequately demonstrate that each of the criterion of 35 U.S.C. § 112 are met. Furthermore, patent scope can be regulated using the requirements of 35 U.S.C. §§ 102, 103 and 112 where the subject matter is determined to be patentable under 35 U.S.C. § 101. See *In re Foster*, 438 F.2d 1011, 1014-16 (C.C.P.A. 1971).

In conclusion, as stated above, Applicants believe that signal claims are patentable subject matter under 35 U.S.C. § 101. If the USPTO ultimately agrees, while we understand that there is no single specific way to properly draft signal claims, we recommend that guidelines specifically acknowledging the patentability of signal claims clearly instruct examiners regarding

acceptable claim language. Claim scope must be clear and must reflect the contents of the specification so that patent owners and patent challengers can avoid the expense and uncertainty of litigation to characterize claim scope after the patent issues.

Claim rejections under 35 USC § 102

Claims 1-37 stand rejected under 35 USC § 102(b) as being anticipated by Secure Authentication for Remote Client Management (IBM TDB No. NNRD41993), 1 March 1999, referred to as “NNRD” hereinafter. Furthermore, claims 1-18, 20-22, 24-28, and 30-37 stand rejected under 35 USC § 102(b) as being anticipated by US Pat 5,826,015, referred to as “Schmidt” hereinafter. Applicant respectfully argues that both NNRD and Schmidt fail to anticipate amended independent claims 1, 13, 15, 20, 27, and 35 and their dependents are traversed with the following remarks.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single reference.¹ Furthermore, the identical invention must be shown in as complete detail as is contained in the claim.²

NNRD

With regards to claims 1, 13, and 15, NNRD does not describe, expressly or inherently, the selection of a bootable image within a local resource of a client computer system, which comprises software to authenticate a software application on a maintenance server.

NNRD describes “firmware [that] allows the server to send to the client a [WOL] packet which tells the client to wake up and boot off the network.”³ “Using this method a bootable image can be sent to a client to execute. This bootable image can contain programs that update the system BIOS, start the install of an operating system, and/or run diagnostics.”⁴ NNRD further discloses “[more] examples include updating firmware, loading and installing a new operating system, running diagnostics, etc.”⁵

¹ *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987).

² *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989).

³ NNRD, lines 29-31.

⁴ NNRD, lines 35-38.

⁵ NNRD, lines 5-7.

Claims 1, 13, and 15 describe a server capable of addressing a security gap that is evident in NNRD. In particular, NNRD instructs the client computer system to boot off a network software source. While NNRD discusses security involved with authenticating the server and the command to boot off the network, NNRD does not address the issue of trustworthiness or authentication of the software on the network that is used to boot the client computer system. In other words, there is a security risk that the software on the network has been tampered with, NNRD does not address this potentiality, and NNRD offers no solution to control the security risk to the client system.

On the other hand, claims 1, 13, and 15, do address this security risk. In claims 1, 13, and 15, the server “select[s] the bootable image that comprises software to determine the trustworthiness of a software application on a maintenance server prior to executing the software application, for the remote client.” The server then “generat[es] a wake-on-LAN packet with a partition identification, the partition identification being associated with a location of the bootable image, to identify the location within a local resource of the remote client.” In claims 1, 13, and 15, the client computer system has control over the trustworthiness of the software used to boot the client system because the software is within a local resource.

Furthermore, the sever “select[s] a bootable image that comprises software to authenticate a software application on a maintenance server.” NNRD does not describe this and does not enable the client computer system to do so. NNRD focuses on authenticating the server and the server’s command with a hardware DES and pre-boot software. Pre-boot software has very limited resources because the memory used to store the pre-boot software, e.g., flash memory, is relatively expensive. NNRD addresses this shortcoming with the hardware DES. However, the hardware DES does not offer flexibility with regards to security measures that is offered from the client computer system after being booted from a trusted software. As specifically described in claims 1, 13, and 15, the server selects software on a local resource of the client “to determine the trustworthiness of a software application on a maintenance server prior to executing the software application.” Thus, Applicant respectfully requests that the rejections be withdrawn and that the claims be allowed.

With regards to claims 20, 27, and 35, NNRD does not describe, expressly or inherently, a client computer system with pre-boot logic “to implement an alternative boot sequence of

booting from a default bootable image to boot from the bootable image at the location within the local resource in response to the presence of the partition identification in the memory location, to execute software to determine the trustworthiness of a software application on a maintenance server prior to executing the software application.” As discussed above, NNRD describes “firmware [that] allows the server to send to the client a [WOL] packet which tells the client to wake up and boot off the network.”⁶ The client computer system receives the location on the network to boot from and, upon authenticating the server and the command from the server, NNRD boots with the software off the network. NNRD describes a significant security gap with regards to the trustworthiness of the software application executed off the network and offers no security measure for addressing this security risk.

On the other hand, claims 20, 27, and 35 describe a capability of client computer systems to boot “from the bootable image at the location within the local resource”, which places security of the software within the security measures implemented by the client computer system. Furthermore, claims 20, 27, and 35, describe a capability of client computer systems to boot “from a default bootable image to boot from the bootable image at the location within the local resource in response to the presence of the partition identification in the memory location”. NNRD does not describe the capability of booting from an alternative location within a local resource. Thus, Applicant respectfully requests that the rejection of amended claims 20, 27, and 35 be withdrawn and that amended claims 20, 27, and 35 be allowed.

Furthermore, claims dependent upon amended claims 1, 13, 15, 20, 27, and 35, incorporate the limitations of claims 1, 13, 15, 20, 27, and 35. Thus, NNRD does not teach all the limitations of these dependent claims so Applicant respectfully suggests that these rejections do not apply and the dependent claims should be allowed.

Schmidt

With regards to claims 1, 13, and 15, Schmidt does not describe, expressly or inherently, the selection of a bootable image within a local resource of a client computer system, which comprises software to authenticate a software application on a maintenance server.

⁶ NNRD, lines 29-31.

Schmidt describes “remote programming of sensitive system resources, like a BIOS”⁷ Schmidt further describes “application software which access the data to generate and transmit wake-up packets to the desktop computers 14 over the network.”⁸ The security measures described in Schmidt determine whether the user is authorized to perform operations from a remote location with via a secure wake-on-LAN packet via, e.g., a password sequence. “The Examiner finds a password to be a form of authentication”.⁹

Claims 1, 13, and 15 describe a server capable of addressing a security gap that is evident in Schmidt. In particular, Schmidt reprograms secure resources such as BIOS based off a password sequence from a remote location. Schmidt does not provide a mechanism with which to authenticate the reprogrammed code, which will executed by the client computer system. Rather than selecting a bootable image within the client computer system, which is a significantly lower security risk and provides measures for the client computer system to authenticate further operations on secure data, Schmidt provides substantially unlimited access via a password sequence. Schmidt does not even address the security risks involved with reprogramming the client computer system after provision of the password sequence. For instance, if the user is a user-authorized software on a server that has been tampered with, the user-authorized software poses a significant risk to all the client computer systems accessed by the invention described in Schmidt.

On the other hand, claims 1, 13, and 15, do address this security risk. In claims 1, 13, and 15, the server “select[s] the bootable image that comprises software to determine the trustworthiness of a software application on a maintenance server prior to executing the software application, for the remote client.” The server then “generat[es] a wake-on-LAN packet with a partition identification, the partition identification being associated with a location of the bootable image, to identify the location within a local resource of the remote client.” In claims 1, 13, and 15, the client computer system has control over the trustworthiness of the software used to boot the client system because the software is within a local resource.

Furthermore, the sever “select[s] a bootable image that comprises software to authenticate a software application on a maintenance server.” Schmidt does not describe this and

⁷ Schmidt, col. 3, lines 28-30.

⁸ Schmidt, col. 13, lines 24-27.

does not enable the client computer system to do so. Schmidt relies on authentication via a password sequence and either booting from the default boot image in the client computer system or reprogramming the boot image and possibly the pre-boot logic, ie, BIOS. Schmidt doesn't address the very limited resources of pre-boot software because the password sequence does not require much overhead. The password sequence does not offer flexibility with regards to security measures that is offered from the client computer system after being booted from a trusted software. As specifically described in claims 1, 13, and 15, the server selects software on a local resource of the client "to determine the trustworthiness of a software application on a maintenance server prior to executing the software application." Thus, Applicant respectfully requests that the rejections be withdrawn and that the claims be allowed.

With regards to claims 20, 27, and 35, Schmidt does not describe, expressly or inherently, a client computer system with pre-boot logic "to implement an alternative boot sequence of booting from a default bootable image to boot from the bootable image at the location within the local resource in response to the presence of the partition identification in the memory location, to execute software to determine the trustworthiness of a software application on a maintenance server prior to executing the software application." As discussed above, Schmidt describes "application software... to generate and transmit wake-up packets to the desktop computers 14 over the network"¹⁰ The client computer system accepts reprogramming upon verification of the password sequence. Thus, Schmidt describes a significant security gap with regards to the trustworthiness of reprogramming remotely over the network and offers no security measure for addressing this security risk.

On the other hand, claims 20, 27, and 35 describe a capability of client computer systems to boot "from the bootable image at the location within the local resource", which places security of the software within the security measures implemented by the client computer system. Furthermore, claims 20, 27, and 35, describe a capability of client computer systems to boot "from a default bootable image to boot from the bootable image at the location within the local resource in response to the presence of the partition identification in the memory location". NNRD does not describe the capability of booting from an alternative location within a local

⁹ Office action, pg. 9, last par.

¹⁰ Schmidt, col. 13, lines 24-27.

resource. Thus, Applicant respectfully requests that the rejection of amended claims 20, 27, and 35 be withdrawn and that amended claims 20, 27, and 35 be allowed.

Furthermore, claims dependent upon amended claims 1, 13, 15, 20, 27, and 35, incorporate the limitations of claims 1, 13, 15, 20, 27, and 35. Thus, Schmidt does not teach all the limitations of these dependent claims so Applicant respectfully suggests that these rejections do not apply and the dependent claims should be allowed.

Double-Patenting rejections

The Office action provisionally rejects claims 1-36 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-35 of co-pending application no. 10/749,584.

Applicant respectfully argues that the claims as amended are more clearly distinct from the claims in the copending application. Further differences can be addressed in the copending application as necessary.

Reservations

Applicant is not conceding in this application that the original claims are not patentable over the art cited by Examiner, as the present claim amendments and cancellations are only for facilitating expeditious prosecution. Applicant respectfully reserves the right to pursue these and other claims in one or more continuations and/or divisional patent applications.

CONCLUSION

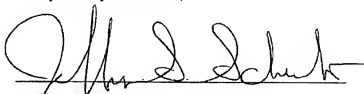
Applicant respectfully responds to the objections and traverses the cited reference in regards to the claim rejections under 35 USC §§ 101 and 102. Accordingly, Applicant believes that this response constitutes a complete response to each of the issues raised in the Office action. In light of the amendments made herein and the accompanying remarks, Applicant believes that the pending claims are in condition for allowance. Thus, Applicant requests that the rejections be withdrawn, pending claims be allowed, and application advance toward issuance. If the Examiner has any questions, comments, or suggestions, the undersigned attorney would welcome and encourage a telephone conference at (512) 288-6635.

The Office is authorized to charge Deposit Account 50-0563 for the extension fee. No other fees are believed due with this paper. However, if any fee is determined to be required, the Office is authorized to charge Deposit Account 50-0563 for any such required fee.

Respectfully submitted,

June 21, 2007

Date



Jeffrey S. Schubert, Reg. No. 43,098
Customer No.: 45670
Schubert Osterrieder & Nickelson PLLC
6013 Cannon Mtn Dr, S14
Austin, Texas 78749
(512) 692-7297 (Telephone)
(512) 301-7301 (Facsimile)
Attorney for Applicant(s)